

On Codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$

A. Melakhessou, K. Guenda, T. A. Gulliver, M. Shi and P. Solé *

Abstract

In this paper we investigate linear codes with complementary dual (LCD) codes and formally self-dual codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$, for q odd. We give conditions on the existence of LCD codes and present construction of formally self-dual codes over R . Further, we give bounds on the minimum distance of LCD codes over \mathbb{F}_q and extend these to codes over R .

1 Introduction

Codes over finite rings have been known for several decades, but interest in these codes increased substantially after the discovery that good non-linear binary codes can be constructed from codes over \mathbb{Z}_4 . Recently, codes over finite non chain rings have been considered. Codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, $v^3 = v$ were introduced by Gao et al. [9], and Shi et al. [26] studied their properties and gave several families of codes over this ring.

Linear codes with complementary dual (LCD) codes over finite fields were first studied by Massey [23] and more recently by Carlet and Guilley [4] and Dougherty et al. [7]. LCD codes can be used to protect information against side channel attacks [4]. When considered over \mathbb{F}_q these codes have the advantage to be easily decoded [23]. This property also applies to LCD codes over R because this ring can be seen as the direct product $\mathbb{F}_q \times \mathbb{F}_q \times \mathbb{F}_q$. Further, LCD codes can be used to obtain optimal entanglement-assisted quantum codes [11].

Formally self-dual codes are an important class of codes because they have weight enumerators that are invariant under the MacWilliams transform, and can have better parameters than self-dual codes [2]. In this paper, LCD and formally self-dual codes are considered over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$ and q is an odd prime power. We give conditions on the existence of LCD codes over this ring. Further, several constructions of

*A. Melakhessou is with Department of Mathematics, University of Batna 2, Algeria, K. Guenda is with the Faculty of Mathematics USTHB, Algeria, T. A. Gulliver is with the Department of Electrical and Computer Engineering, University of Victoria, Canada, M. Shi is with the School of Mathematical Sciences, Anhui University, P.R. China, and P. Solé is with the Department of Mathematics, Université de Vincennes - Paris 8, France.

LCD codes are given, in particular from weighing matrices. Constructions of formally self-dual codes over R are also presented. In addition, bounds on the minimum distance of LCD codes over the finite field \mathbb{F}_q are given and extended to codes over R .

The remainder of this paper is organized as follows. Section 2 provides some preliminary results regarding the finite ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. The Lee weights of the elements of R are defined, and a Gray map is introduced. This map leads to some useful results on linear codes over R . We investigate the relationship between the dual and Gray image of codes. Section 3 considers LCD codes over R . Necessary and sufficient conditions on the existence of LCD codes over R are given, and LCD codes are constructed from weighing matrices. Tables of LCD codes up to length 40 are given which are obtained from skew matrices and conference matrices over the finite field \mathbb{F}_p where p is a prime number such that $3 < p \leq 23$. In Section 4, we present three constructions of formally self-dual codes over R . Further, LCD codes are constructed which are also formally self-dual. In Section 5 we give bounds on the minimum distance of LCD codes over \mathbb{F}_q , and these bounds are extended to free LCD codes over R .

2 Preliminaries

In this section, we present some basic results on linear codes over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$ and q is odd [9, 26]. The ring R is equivalent to the ring $\frac{\mathbb{F}_q[v]}{\langle v^3 - v \rangle}$. This shows that R is a finite commutative, principal ring with the following non-trivial maximal ideals

$$\langle v \rangle, \langle 1 - v \rangle, \langle 1 + v \rangle.$$

Hence by the Chinese Remainder Theorem we have

$$R = R/\langle v \rangle \oplus R/\langle 1 - v \rangle \oplus R/\langle 1 + v \rangle. \quad (1)$$

It is convenient to write the decomposition given in (1) using orthogonal idempotents in R which is given by

$$R = \eta_1 R \oplus \eta_2 R \oplus \eta_3 R = \eta_1 \mathbb{F}_q \oplus \eta_2 \mathbb{F}_q \oplus \eta_3 \mathbb{F}_q, \quad (2)$$

where $\eta_1 = 1 - v^2$, $\eta_2 = \frac{v+v^2}{2}$, and $\eta_3 = \frac{v^2-v}{2}$. Each element r of R can be expressed uniquely as $r = a_0 + va_1 + v^2a_2$, where $a_i \in \mathbb{F}_q, i = 0, 1, 2$.

A linear code C of length n over R is an R -submodule of R^n . An element of C is called a codeword of C . A generator matrix of C is a matrix whose rows generate C . The Hamming weight $w_H(c)$ of a codeword c is the number of nonzero components in c . The Euclidean inner product is

$$x \cdot y = x_0y_0 + x_1y_1 + \dots + x_{n-1}y_{n-1},$$

where $x, y \in R^n$. The dual code C^\perp of C with respect to the Euclidean inner product is defined as

$$C^\perp = \{x \in R^n; x \cdot y = 0, \forall y \in C\}.$$

A code C is called self-dual if $C = C^\perp$ and C is called self-orthogonal if $C \subseteq C^\perp$.

For a linear code C of length n over R , define

$$\begin{aligned} C_1 &= \{a \in \mathbb{F}_q^n; \exists b, c \in \mathbb{F}_q^n; \eta_1 a + \eta_2 b + \eta_3 c \in C\}, \\ C_2 &= \{b \in \mathbb{F}_q^n; \exists a, c \in \mathbb{F}_q^n; \eta_1 a + \eta_2 b + \eta_3 c \in C\}, \\ C_3 &= \{c \in \mathbb{F}_q^n; \exists a, b \in \mathbb{F}_q^n; \eta_1 a + \eta_2 b + \eta_3 c \in C\}. \end{aligned}$$

It is clear that C_1 , C_2 and C_3 are linear codes of length n over \mathbb{F}_q . A direct consequence of the ring decomposition of R in (2) is that a linear code C over R can be uniquely expressed as

$$C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3. \quad (3)$$

Moreover, from (3) and the definition of the dual code we have that

$$C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp. \quad (4)$$

Further, C is self-dual if and only if C_1 , C_2 and C_3 are self-dual over \mathbb{F}_q . If G_1 , G_2 and G_3 are generator matrices of C_1 , C_2 and C_3 , respectively, then

$$G = \begin{bmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \end{bmatrix}, \quad (5)$$

is a generator matrix of C . Often when working with codes over rings, an image to the underlying field is employed. For the ring R considered in this paper, a Gray map is defined as follows.

Definition 2.1 *The Gray map Ψ from R^n to \mathbb{F}_q^{3n} is defined by*

$$\begin{aligned} \Psi : R^n &\rightarrow \mathbb{F}_q^{3n} \\ (r_0, r_1, \dots, r_{n-1}) &\mapsto (a_0, a_0 + b_0 + c_0, a_0 - b_0 + c_0, \dots, a_{n-1} + b_{n-1} + c_{n-1}, a_{n-1} - b_{n-1} + c_{n-1}), \end{aligned}$$

where $r_i = a_i + vb_i + v^2c_i, i = 0, 1, \dots, n-1$.

For $r = a + vb + v^2c$ in R , the Lee weight of r is defined as

$$w_L(a + vb + v^2c) = w_H(a, a + b + c, a - b + c),$$

where w_H denotes the Hamming weight of v over \mathbb{F}_q . Let d_H denote the minimum Hamming distance of a code C . For a codeword $c = (c_0, c_1, \dots, c_{n-1})$, the Lee weight is defined as $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$ and the Lee distance between codewords c and c' is defined as $d_L(c, c') = w_L(c - c')$. The minimum Lee distance of a code C is then $d_L(C) = \min d_L(c, c'), c \neq c', \forall c, c' \in C$.

Definition 2.2 A linear code C of length n over R and minimum Lee distance d_L is called an $[n, |C|, d_L]_R$ code. Further if it is with minimum Hamming distance d_H , then it is denoted $[n, |C|, d_H]_R$. If C has minimum Lee distance d_L and is a free R -submodule that is isomorphic as a module to R^k , then the integer k is called the rank of C and the code is denoted as $[n, k, d_L]_R$.

Proposition 2.3 [26] Let C be an $[n, |C|, d_L]_R$ code. Then $\Psi(C)$ is a $[3n, k, d = d_L]$ linear code over \mathbb{F}_q . Further, if C^\perp is the dual of C , then $\Psi(C)^\perp = \Psi(C^\perp)$.

Remark 2.4 If there exists an $[n, k, d_H]$ code C over \mathbb{F}_q , then there exists a $[n, k, d_H]_R$ code $\mathcal{C} = \eta_1 C \oplus \eta_2 C \oplus \eta_3 C$.

Lemma 2.5 [26] If C is a linear code of length n over R with generator matrix G , then

$$\Psi(G) = \begin{bmatrix} \Psi(\eta_1 G_1) \\ \Psi(\eta_2 G_2) \\ \Psi(\eta_3 G_3) \end{bmatrix} = \begin{bmatrix} G_1 & 0 & 0 \\ 0 & G_2 & 0 \\ 0 & 0 & G_3 \end{bmatrix}, \quad (6)$$

and $d_H(\Psi(C)) = \min\{d_H(C_1), d_H(C_2), d_H(C_3)\}$.

We now give some useful results on cyclic codes over R . A code C is said to be cyclic if it satisfies

$$(c_{n-1}, c_0, \dots, c_{n-2}) \in C, \text{ whenever } (c_0, c_1, \dots, c_{n-1}) \in C.$$

It is well known that cyclic codes of length n over R can be considered as ideals in the quotient ring $\frac{R[x]}{\langle x^n - 1 \rangle}$ via the following R -module isomorphism

$$\begin{aligned} R^n &\rightarrow R[x] / \langle x^n - 1 \rangle \\ (c_0, c_1, \dots, c_{n-1}) &\mapsto c_0 + c_1 x + \dots + c_{n-1} x^{n-1} \end{aligned}$$

Definition 2.6 The reciprocal of the polynomial $h(x) = h_0 + h_1 x + \dots + h_k x^k$ is defined as

$$h^*(x) = x^{\deg(h(x))} h(x^{-1}).$$

If $h(x) = h^*(x)$, then the polynomial $h(x)$ is called self-reciprocal.

Proposition 2.7 [9] Let C be a cyclic code of length n over R . Then there exist polynomials $f_i(x)$ which are divisors of $x^n - 1$ in $\mathbb{F}_q[x]$ such that $C = \langle \eta_1 f_1(x), \eta_2 f_2(x), \eta_3 f_3(x) \rangle$ and $|C| = q^{3n - \deg(f_1(x) + f_2(x) + f_3(x))}$. Further

$$C^\perp = \langle \eta_1 h_1^*(x), \eta_2 h_2^*(x), \eta_3 h_3^*(x) \rangle,$$

where $h_i(x) \in \mathbb{F}_q[x]$ such that $x^n - 1 = f_1(x)h_1(x) = f_2(x)h_2(x) = f_3(x)h_3(x)$.

Proposition 2.8 *There is no cyclic self-dual cyclic code of length n over R .*

Proof. We know that $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$. From [16, Theorem 1] we have that C_1 , C_2 and C_3 are self-dual cyclic codes over \mathbb{F}_q if and only if q is a power of 2 and n is even. Since we assumed that q is odd, the result then follows. ■

3 LCD Codes over R

A linear codes with complementary dual (LCD) code is defined as a linear code C whose dual code C^\perp satisfies

$$C \cap C^\perp = \{0\}.$$

LCD codes have been shown to provide an optimum linear coding solution [23].

For LCD codes over R , we have the following result.

Theorem 3.1 *A code $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ of length n over R is an LCD code if and only if C_1 , C_2 and C_3 are LCD codes over \mathbb{F}_q .*

Proof. A linear code $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ has dual code $C^\perp = \eta_1 C_1 \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp$. We have that $C \cap C^\perp = \eta_1(C_1 \cap C_1^\perp) \oplus \eta_2(C_2 \cap C_2^\perp) \oplus \eta_3(C_3 \cap C_3^\perp)$. Due to the direct sum we have $C \cap C^\perp = \{0\}$ if and only if $C_i \cap C_i^\perp = \{0\}$, for $i = 1, 2, 3$. Thus C is an LCD code. ■

Theorem 3.2 *If C is an LCD code over \mathbb{F}_q , then $\mathcal{C} = \eta_1 C \oplus \eta_2 C \oplus \eta_3 C$ is an LCD code over R . If \mathcal{C} is an LCD code of length n over R , then $\Psi(\mathcal{C})$ is an LCD code of length $3n$ over \mathbb{F}_q .*

Proof. The first part is deduced from Theorem 3.1. From Proposition 2.3, we have that $\Psi(C)^\perp = \Psi(C^\perp)$. Since Ψ is bijective and $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$, the result follows. ■

Next we give a necessary and sufficient condition on the existence of LCD codes over R . First we require the following result due to Massey [23].

Proposition 3.3 *If G is a generator matrix for an $[n, k]$ linear code C over \mathbb{F}_q , then C is an LCD code if and only if the $k \times k$ matrix GG^t is nonsingular.*

Theorem 3.4 *If G is a generator matrix for a linear code C over R , then C is an LCD code if and only if GG^t is nonsingular.*

Proof. The generator matrix of C can be expressed in canonical form as

$$G = \begin{bmatrix} \eta_1 G_1 \\ \eta_2 G_2 \\ \eta_3 G_3 \end{bmatrix}. \quad (7)$$

Since the η_i are orthogonal idempotents, a simple calculation gives

$$GG^t = \begin{bmatrix} \eta_1 G_1 G_1^t & 0 & 0 \\ 0 & \eta_2 G_2 G_2^t & 0 \\ 0 & 0 & \eta_3 G_3 G_3^t \end{bmatrix}. \quad (8)$$

From Proposition 3.3 a necessary and sufficient condition for a code over \mathbb{F}_q with generator matrix G_i to be LCD is that $G_i G_i^t$ be non singular. Hence the proof follows from the generator matrix given in (7). \blacksquare

We now give conditions on the existence of cyclic LCD codes over R using the generator polynomial. This is an extension of the following result due to Massey [23].

Lemma 3.5 *Let C be a cyclic code over \mathbb{F}_q generated by $f(x)$. Then C is LCD if and only if $f(x)$ is self-reciprocal.*

Theorem 3.6 *A cyclic code $C = \langle \eta_1 f_1(x), \eta_2 f_2(x), \eta_3 f_3(x) \rangle$, is an LCD code over R if and only if for all $1 \leq i \leq 3$, $f_i(x)$ is a self-reciprocal polynomial.*

Proof. The result follows from Proposition 2.7 and Lemma 3.5. \blacksquare

3.1 Existence of LCD Codes over R

In this section, we show that LCD codes are an abundant class of codes over R .

3.2 LCD Codes from Weighing Matrices

In [7], the authors constructed LCD codes from orthogonal matrices and left the existence of LCD codes from other classes of combinatorial objects as an open problem. Thus, in this section we construct LCD codes over \mathbb{F}_q and R from weighing matrices. We start with the following definition.

Definition 3.7 *A weighing matrix $W_{n,k}$ of order n and weight k is an $n \times n$ $(0, 1, -1)$ -matrix such that $WW^t = kI_n$, $k \leq n$. A weighing matrix $W_{n,n}$, respectively $W_{n,n-1}$, is called a Hadamard matrix, respectively conference matrix. A matrix W is symmetric if $W = W^t$, and W is skew-symmetric (or skew) if $W = -W^t$.*

Tables of weighing matrices are given in [5]. Weighing matrices have been used to construct self-dual codes [1]. The following results show that it is also possible to construct LCD codes from weighing matrices.

Proposition 3.8 *Let $W_{n,k}$ be a weighing matrix of order n and weight k . We have the following results.*

(i) *Let α be a nonzero element of \mathbb{F}_q such that $\alpha^2 + k \neq 0 \pmod{q}$. Then the matrix*

$$G = [\alpha I_n \mid W_{n,k}] \quad (9)$$

generates an LCD $[2n, n]$ code over \mathbb{F}_q .

(ii) *Let $W_{n,k}$ be a skew weighing matrix of order n , and α and β nonzero elements of \mathbb{F}_q such that $\alpha^2 + \beta^2 + k \neq 0 \pmod{q}$. Then the matrix*

$$G = [\alpha I_n \mid \beta I_n + W_{n,k}] \quad (10)$$

generates a $[2n, n]$ LCD code over \mathbb{F}_q .

Proof. The result follows from Definition 3.7 and Proposition 3.3. ■
From Remark 2.4 and Proposition 3.8 we have the following result.

Corollary 3.9 *Under the condition of Proposition 3.8, the matrix*

$$\mathcal{G} = \begin{bmatrix} \eta_1 G \\ \eta_2 G \\ \eta_3 G \end{bmatrix}, \quad (11)$$

is the generator matrix of a $[2n, n]$ LCD code over R .

Example 3.10 *Let $q = 3$, $n = 6$, and $\alpha = 2$ so that $\alpha^2 + 4 \neq 0 \pmod{3}$. Then for the weighing matrix given by*

$$W_{6,4} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 \\ -1 & 0 & 0 & 1 & -1 & 1 \\ -1 & 0 & 0 & -1 & 1 & 1 \\ -1 & -1 & 1 & 0 & 0 & -1 \\ -1 & 1 & -1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 1 & 1 & 0 \end{pmatrix},$$

$G = [2I_6 \mid W_{6,4}]$ *generates a $[12, 6, 5]$ LCD code over \mathbb{F}_3 .*

Next we show that if q is odd there always exists a suitable matrix to construct an LCD code.

Theorem 3.11 [20, Theorem 7.32] Assume $q \equiv 3 \pmod{4}$, η be the quadratic character of \mathbb{F}_q and $b_{ij} = \eta(j - i)$ for $1 \leq i, j \leq q$, $i \neq j$. Then we have a Hadamard matrix given by

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & -1 & b_{12} & b_{13} & \dots & b_{1q} \\ 1 & b_{21} & -1 & b_{23} & \dots & b_{2q} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & b_{q1} & b_{q2} & b_{q3} & \dots & -1 \end{bmatrix}. \quad (12)$$

Corollary 3.12 For all nonzero $\alpha \in \mathbb{F}_q$ such that $q \equiv 3 \pmod{4}$, the code generated by

$$G = [\alpha I_{q+1} \mid H], \quad (13)$$

where H is the Hadamard matrix of order $q + 1$ given in (12), is an LCD code over \mathbb{F}_q of length $2(q + 1)$.

Proof. If $q \equiv 3 \pmod{4}$, then from [10, Lemma 3.3] $\alpha^2 + 1 = 0$ has no solution in \mathbb{F}_q . The result then follows from Proposition 3.8 and Theorem 3.11. \blacksquare

Example 3.13 From Corollary 3.12, the following Hadamard matrix over \mathbb{F}_3

$$H_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{bmatrix}$$

gives an $[8, 4, 4]$ LCD code over \mathbb{F}_3 . According to [12] this is an optimal code.

Theorem 3.14 [24, p. 56] Assume $q \equiv 1 \pmod{4}$, η be the quadratic character of \mathbb{F}_q and $b_{ij} = \eta(j - i)$ for $1 \leq i, j \leq q$. Then we have a symmetric conference matrix given by

$$Q = \begin{bmatrix} 0 & 1 & 1 & 1 & \dots & 1 \\ 1 & b_{11} & b_{12} & b_{13} & \dots & b_{1q} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & b_{q1} & b_{q2} & b_{q3} & \dots & b_{qq} \end{bmatrix}. \quad (14)$$

Corollary 3.15 For all nonzero $\alpha \in \mathbb{F}_q$ such that $q \equiv 1 \pmod{4}$, the code generated by

$$G = [\alpha I_{q+1} \mid Q], \quad (15)$$

where Q is the conference matrix of order $q + 1$ given in (14), is an LCD code over \mathbb{F}_q of length $2(q + 1)$.

Table 1: LCD codes from Proposition 3.8 using conference matrices with $N = 8, 12$ and 16 .

p	α	β	d	α	d	α	β	d
5	2	1	4	1	6	2	1	7
7	1	3	5	1	6	2	1	7
11	1	2	5	1	6	1	0	7
13	2	3	5	1	6	1	6	7
17	2	8	5	1	6	2	3	7
19	1	8	5	1	6	2	7	7
23	3	4	5	1	6	3	0	7

Table 2: LCD codes from Proposition 3.8 using conference matrices with $N = 20, 24$ and 28 .

p	α	d	α	β	d	α	d
5	2	8	1	0	9	1	10
7	1	8	2	3	9	2	10
11	1	8	1	0	9	1	10
13	1	8	5	5	9	1	10
17	1	8	1	6	9	1	10
19	1	8	2	8	9	1	10
23	1	8	1	0	9	1	10

Proof. The result follows from Theorem 3.14 and Proposition 3.3. ■

In [1] the authors constructed self-dual codes from conference matrices. We note that if $\alpha^2 + k = 0$ has a solution, the matrix $[\alpha I_n \mid W_{n,k}]$ generates a self-dual code over \mathbb{F}_q . Then if there exists $\alpha' \neq 0$ such that $\alpha'^2 + k \neq 0$, from Proposition 3.8 $[\alpha' I_n \mid W_{n,k}]$ generates an LCD code with the same parameters as the self-dual code. This result also holds for the minimum distance of LCD codes generated by $G = [\alpha' I_n \mid \beta I_n + W_{n,k}]$. It is easy to verify that whenever we have a skew matrix $W_{n,k}$, we can construct a skew matrix $W_{2n,2k+1}$, where

$$W_{2n,2k+1} = \begin{bmatrix} W_{n,k} & -W_{n,k} - I \\ W_{n,k} + I & W_{n,k} \end{bmatrix}. \quad (16)$$

The above results were used to construct the LCD codes over \mathbb{F}_p , p prime, $3 < p \leq 23$, given in Tables 1-4. It is worth noting that for many parameters a self-dual code cannot be constructed from weighing matrices, whereas for the same parameters (except for the case $p = 3$), it was always possible to construct LCD codes.

Table 3: LCD codes from Proposition 3.8 using conference matrices with $N = 32, 36$ and 40.

p	α	β	d	α	d	α	β	d
5	2	2	10	1	12	2	0	13
7	1	3	11	1	12	1	0	13
11	1	5	11	1	12	1	0	13
13	2	6	11	1	12	1	4	13
17	1	0	11	1	12	1	0	13
19	1	0	11	1	12	1	0	13
23	1	2	11	1	12	1	0	13

Table 4: LCD codes from Proposition 3.8 using the skew matrix $W_{14,9}$.

p	α	β	d
5	2	0	8
7	2	2	10
11	1	3	10
13	2	4	11
17	1	2	11
19	2	3	11
23	2	6	11

3.3 General Construction of LCD Codes

We start with the following lemma.

Lemma 3.16 *If $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ with $q = p^r$ a power of an odd prime, then the following hold:*

- (i) *there exists $\alpha \in R$ such that $\alpha^2 + 1 = 0$ if $q \equiv 1 \pmod{4}$,*
- (ii) *there exist $\alpha, \beta \in R$ such that $\alpha^2 + \beta^2 + 1 = 0$ if $q \equiv 3 \pmod{4}$, and*
- (iii) *for every q there exist $\alpha, \beta, \gamma, \delta \in R$ such that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 0$ in R .*

Proof. It is easy to show that if there exist solutions over \mathbb{F}_q for cases (i)-(iii), then these solutions also hold over R since \mathbb{F}_q is a subring of R . Hence we only need to show that these solutions exist over \mathbb{F}_q . From [10, Lemma 3.3], if $q \equiv 1 \pmod{4}$ then -1 is a square in \mathbb{F}_q , which proves (i). From [15, p. 281], if $q \equiv 3 \pmod{4}$ then there exist $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 + \beta^2 + 1 = 0$, which proves (ii). From [13, Theorem 370], we have that every prime is the sum of four squares. Since $q = p^r$ and $p = 0$ in R this proves (iii). ■

The next result shows that it is always possible to construct LCD codes over R .

Theorem 3.17 *If P is the generator matrix of a self-dual code over R , then the generator matrix $G = [I \mid P]$ generates an LCD code over R . If $G = [I \mid P]$ is the generator matrix of a linear code over R , then the following hold.*

- (i) *If $q \equiv 1 \pmod{4}$ and $\alpha^2 + 1 = 0$, then the code over R with generator matrix $G' = [I \mid P \mid \alpha P]$ generates an LCD code over R .*
- (ii) *If $q \equiv 3 \pmod{4}$ and $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^2 + \beta^2 + 1 = 0$, then $G' = [I \mid P \mid \alpha P \mid \beta P]$ generates an LCD code over R .*
- (iii) *If $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$ with $q = p^r$, then $G' = [I \mid P \mid \alpha P \mid \beta P \mid \delta P \mid \gamma P]$ such that $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = p$ generates an LCD code over R .*

Proof. Part (i) is just a verification. The other parts follow from Lemma 3.16. ■

4 Construction of Formally Self-Dual Codes over R

Recall that a code C is called formally self-dual if C and C^\perp have the same weight enumerator. Codes which are equivalent to their dual are called isodual codes, and isodual codes are also formally self-dual. In this section, we present three constructions of formally self-dual codes over R . First, we give the following result which links formally self-dual codes over R to formally self-dual codes over \mathbb{F}_q .

Theorem 4.1 *If C is a formally self-dual code over R , then the image under the corresponding Gray map is a formally self-dual code.*

Proof. The result follows from Theorem 2.7 and the fact that the Gray map is an isometry. ■

An $n \times n$ square matrix M is called λ -circulant of order n if it has the following form

$$M = \begin{bmatrix} M_{11} & M_{12} & M_{13} & \dots & M_{1n} \\ \lambda M_{1n} & M_{11} & M_{12} & \dots & M_{1n-1} \\ \lambda M_{1n-1} & \lambda M_{1n} & M_{11} & \dots & M_{1n-2} \\ \vdots & \vdots & \vdots & \vdots & \\ \lambda M_{12} & \lambda M_{13} & \lambda M_{14} & \dots & M_{11} \end{bmatrix}.$$

If $\lambda = 1$ this matrix is circulant and there is a vast literature on double circulant and bordered double circulant self-dual codes [2].

The proof of the next theorem is the same as that for [2, Theorem 6.1] given over the ring $\mathbb{F}_q + v\mathbb{F}_q$. It is given here for completeness.

Theorem 4.2 *Let M be a λ -circulant matrix over R of order n . Then the code generated by $G = [I_n \mid M]$ is a formally self-dual code over R .*

Proof. Let C be the code generated by $G = [I_n \mid M]$ and C' the code generated by $G' = [M^t \mid -I_n]$. It is easy to verify that the codes C and C' are orthogonal codes, and since they both have rank n , $C' = C^\perp$. Let C'' be the code generated by $G'' = [M^t \mid I_n]$. Since $wt(a) = wt(-a)$ for any a in R , the codes C' and C'' have the same weight enumerator. In order to complete the proof, we show that C'' is equivalent to C , therefore C is formally self-dual. Let σ be the permutation

$$\sigma = (1, n)(2, n-1) \dots (k-1, n-k+2)(k, n-k+1),$$

where $k = n/2$. If M' is the matrix obtained by applying σ on the rows of M and M'' is the matrix obtained by applying σ on the columns of M' , then $M'' = M^t$. Hence, M and M^t are equivalent. Similarly, by applying a suitable column permutation we obtain that G and G'' are equivalent. Thus, C and C'' are equivalent and therefore C is formally self-dual. ■

Example 4.3 *Let $q = 3$, $n = 4$, $\lambda = 1 + v$ and M be the following λ -circulant matrix*

$$M = \begin{bmatrix} 2v + 2v^2 & 2 + v + v^2 & 1 + 2v & 2 \\ 2 + 2v & 2v + 2v^2 & 2 + 2v + 2v^2 & 1 + 2v \\ 1 + 2v^2 & 2 + 2v & 2v + 2v^2 & 2 + 2v + 2v^2 \\ 2 + v^2 & 1 + 2v^2 & 2 + 2v & 2v + 2v^2 \end{bmatrix}.$$

Then $G = [I_4 \mid M]$ generates a formally self-dual code of length 8 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$. The Gray image of this code is a $[24, 12, 9]$ formally self-dual code over \mathbb{F}_3 . This is an optimal code.

Example 4.4 Let $q = 5$, $n = 3$, $\lambda = 2 + v$ and M be the following λ -circulant matrix

$$M = \begin{bmatrix} 3v + 2v^2 & 4v & 3 + 2v \\ 1 + 2v + 2v^2 & 3v + 2v^2 & 4v \\ 3v + 4v^2 & 1 + 2v + 2v^2 & 3v + 2v^2 \end{bmatrix}.$$

Then $[I_3 \mid M]$ generates a formally self-dual code of length 6 over $\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5$. The Gray image of this code is an $[18, 9, 7]$ formally self-dual code over \mathbb{F}_5 .

Theorem 4.5 Let M be an $(n-1) \times (n-1)$ λ -circulant matrix. Then the code generated by

$$G = \left[I_n \left| \begin{array}{cccc} \alpha & \omega & \dots & \omega \\ \omega & & & \\ \vdots & & M & \\ \omega & & & \end{array} \right. \right]$$

where $\alpha, \omega \in R$, is a formally self-dual code over R .

Proof. The proof is similar to that of Theorem 4.2. ■

Example 4.6 Let $q = 3$, $\alpha = 2 + v + 2v^2$, $\omega = 2 + 2v$, $\lambda = 1 + v^2$, $n = 3$ and

$$M = \begin{bmatrix} 2 & 1 + v \\ 1 + 2v + v^2 & 2 \end{bmatrix}.$$

Then

$$G = \begin{bmatrix} 1 & 0 & 0 & 2 + v + 2v^2 & 2 + 2v & 2 + 2v \\ 0 & 1 & 0 & 2 + 2v & 2 & 1 + v \\ 0 & 0 & 1 & 2 + 2v & 1 + 2v + v^2 & 2 \end{bmatrix},$$

generates a formally self-dual code of length 6 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$. The Gray image of this code is an $[18, 9, 6]$ formally self-dual code over \mathbb{F}_3 . This is an optimal code.

Using a proof similar to that of Theorem 4.2, we have the following construction of formally self-dual codes over R .

Theorem 4.7 Let A be an $n \times n$ matrix over R such that $A^t = A$. Then the code generated by $G = [I_n \mid A]$ is a formally self-dual code over R of length $2n$.

Example 4.8 Let $q = 5$, $n = 3$, and A be the matrix

$$A = \begin{bmatrix} 4v + 1 & v + v^2 & 4 + 4v \\ v + v^2 & 4v & 1 + v \\ 4 + 4v & 1 + v & 1 + v \end{bmatrix}.$$

We have that $A = A^t$, so $[I_3 \mid A]$ generates a formally self-dual code of length 6 over $\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5$. The Gray image of this code is an $[18, 9, 7]$ formally self-dual code over \mathbb{F}_5 .

Example 4.9 Let $q = 9$, $n = 5$, and A be the matrix

$$A = \begin{bmatrix} 0 & v & 8 + v & 1 + 8v + 8v^2 & 8v + 8v^2 \\ v & 8v + 8v^2 & 8 & 1 + v & 1 + v^2 \\ 8 + v & 8 & 8v^2 & 8 + v + v^2 & 1 + 8v \\ 1 + 8v + 8v^2 & 1 + v & 8 + v + v^2 & 1 & v \\ 8v + 8v^2 & 1 + v^2 & 1 + 8v & v & 8 \end{bmatrix}.$$

We have that $A = A^t$, so $[I_5 \mid A]$ generates a formally self-dual code of length 10 over $\mathbb{F}_9 + v\mathbb{F}_9 + v^9\mathbb{F}_9$. The Gray image of this code is a $[30, 15, 12]$ formally self-dual code over \mathbb{F}_9 .

Proposition 4.10 Let C_1 , C_2 and C_3 be linear codes of length n over \mathbb{F}_q . C_1 , C_2 and C_3 are isodual codes if and only if $C = \eta_1 C_1 \oplus \eta_2 C_2 \oplus \eta_3 C_3$ is an isodual code of length n over R .

Proof. Let τ_1 , τ_2 , and τ_3 be monomial permutations such that $\tau_1(C_1) = C_1^\perp$, $\tau_2(C_2) = C_2^\perp$ and $\tau_3(C_3) = C_3^\perp$. Then $\eta_1 \tau_1(C_1) \oplus \eta_2 \tau_2(C_2) \oplus \eta_3 \tau_3(C_3) = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp$. Since $C^\perp = \eta_1 C_1^\perp \oplus \eta_2 C_2^\perp \oplus \eta_3 C_3^\perp$, it follows that C is equivalent to C^\perp . ■

4.1 Construction of LCD Formally Self-Dual Codes over R

LCD formally self-dual codes over R are constructed in this subsection.

Theorem 4.11 With the same assumptions as in Theorem 4.2, the matrix $G = [I_n \mid M]$ generates an LCD formally self-dual code over R if and only if GG^t is nonsingular.

Proof. The result follows from Theorem 4.2 and Theorem 3.4. ■

Example 4.12 Let $q = 5$, $n = 4$, $\lambda = 4v^2$ and M be the following λ -circulant matrix

$$M = \begin{bmatrix} 2v^2 & 0 & v & 0 \\ 0 & 2v^2 & 0 & v \\ 4v & 0 & 2v^2 & 0 \\ 0 & 4v & 0 & 2v^2 \end{bmatrix}.$$

It is easily determined that GG^t is nonsingular. Thus, $G = [I_4 | M]$ generates an LCD formally self-dual code of length 8 over $\mathbb{F}_5 + v\mathbb{F}_5 + v^2\mathbb{F}_5$.

Theorem 4.13 With the same assumptions as in Theorem 4.5, the code generated by

$$G = \left[I_n \left| \begin{array}{cccc} \alpha & \omega & \dots & \omega \\ \omega & & & \\ \vdots & & M & \\ \omega & & & \end{array} \right. \right],$$

is an LCD formally self-dual code over R if and only if GG^t is nonsingular.

Example 4.14 Let $q = 3$, $n = 3$, $\lambda = v^2$ and M be the following λ -circulant matrix

$$M = \begin{bmatrix} v & v \\ v & v \end{bmatrix}.$$

If $\alpha = v$ and $\omega = v^2$, it is easily determined that for the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & v & v^2 & v^2 \\ 0 & 1 & 0 & v^2 & v & v \\ 0 & 0 & 1 & v^2 & v & v \end{bmatrix},$$

GG^t is nonsingular. Then G generates an LCD formally self-dual code of length 6 over $\mathbb{F}_3 + v\mathbb{F}_3 + v^2\mathbb{F}_3$.

Theorem 4.15 With the same assumptions as in Theorem 4.7, the code generated by $G = [I_n | A]$ is an LCD formally self-dual code over R if and only if GG^t is nonsingular.

Proof. From Theorem 4.7, we know that G generates a formally self-dual code. To prove that G generates an LCD codes we apply the conditions of Theorem 3.4 on the matrix $G = [I_n | A]$. ■

5 Bounds on LCD Codes

Bounds on codes are important for the combinatorial properties of the codewords as it was shown in [3]. In this section we will give some bounds on LCD codes over fields and the ring R . When dealing with codes over \mathbb{F}_q , q may be odd or even. While, when we are over the ring R , q must be odd as assumed in the begin of the paper.

We begin with the following bound which was given by Dougherty et al. [7]

$$LCD[n, k]_q := \max\{d; \text{there exists an } [n, k, d]_q \text{ LCD code}\}.$$

They also gave estimates and results for this bound. For linear codes over \mathbb{F}_q , we have the following bound

$$\mathcal{B}(n, k)_q := \max\{d; \text{there exists an } [n, k, d]_q \text{ code}\}.$$

The next result gives an upper bound on d for an LCD code over \mathbb{F}_q

Proposition 5.1 *If an $[n, n/2, d]_q$ self-dual code C exists, then $LCD[3n/2, n/2]_q \geq d$. In particular, if C is an extremal self-dual code over \mathbb{F}_2 , then $LCD[3n/2, n/2]_2 \geq \frac{4n}{24} + 4$ if $n \not\equiv 22 \pmod{24}$, and $LCD[3n/2, n/2]_2 \geq \frac{4n}{24} + 6$ if $n \equiv 22 \pmod{24}$. For \mathbb{F}_3 and $n \equiv 0 \pmod{4}$, $LCD[3n/2, n/2]_3 \geq 3n/12 + 3$.*

Proof. If there exists an $[n, n/2, d]_q$ self-dual code with generator matrix P , then the matrix $G = [I \mid P]$ satisfies $GG^t = I$, and hence by Proposition 3.3 G generates an LCD code with parameters $[3n/2, n/2, \geq d]$. In the binary case, the bound given corresponds to the condition on extremal binary self-dual codes given in [14, Chap. 9]. In the ternary case, the bound corresponds to the condition on extremal ternary self-dual codes given in [14, Chap. 9]. ■

The proof of the following result follows from Theorem 3.17 and the Singleton bound.

Proposition 5.2 *If there exists an $[n, k, d]_q$ code over \mathbb{F}_q , then*

$$\begin{aligned} d &\leq LCD[n+k, k]_q \leq \mathcal{B}(n+k, k)_q \leq n+1 \text{ if } q = 2^m, \\ d &\leq LCD[2n+k, k]_q \leq \mathcal{B}(2n+k, k)_q \leq 2n+1 \text{ if } q \equiv 1 \pmod{4}, \\ d &\leq LCD[3n+k, k]_q \leq \mathcal{B}(3n+k, k)_q \leq 3n+1 \text{ if } q \equiv 3 \pmod{4}, \\ d &\leq LCD[4n+k, k]_q \leq \mathcal{B}(4n+k, k)_q \leq 4n+1 \text{ for all } q. \end{aligned}$$

Proposition 5.3 *If q is odd, then $LCD[q+1, q-2\mu]_q = B(q+1, q-2\mu)_q = 2\mu+2$, for $1 \leq \mu \leq \frac{q-1}{2}$.*

If q is even, then $LCD[q+1, q-1-2\mu]_q = B(q+1, q-1-2\mu) = 2\mu+3$, for $1 \leq \mu \leq \frac{q-1}{2}-1$.

Proof. From [8, Theorem 8], if $q + 1 - k$ is odd (this case correspond to q and k both even or odd), then the cyclic code generated by the polynomial $g_1(x) = \prod_{i=-\mu}^{\mu} (x - \alpha^i)$ is a $[q + 1, q - 2\mu, 2\mu + 2]_q$ maximum distance separable (MDS) cyclic code. Since $g_1(x)$ is self-reciprocal, from Lemma 3.5 the code is LCD. Since the code is also MDS, the result follows.

If q is even and k is odd, then the polynomial $g_2(x) = \prod_{i=q/2-\mu}^{q/2} (x - \alpha^i)(x - \alpha^{-i})$ generates a $[q + 1, q - 1 - 2\mu, 2\mu + 3]_q$ MDS cyclic code from [8, Theorem 8]. Since $g_2(x)$ is self-reciprocal, the code is LCD by Lemma 3.5. The result then follows since the code is MDS. \blacksquare

For codes over R , define the bound

$$LCD[n, k]_R := \max\{d; \text{ there exists an } [n, k, d_H]_R \text{ free LCD code over } R\}.$$

From Remark 2.4, we have the following bound

$$LCD[n, k]_R \geq LCD[n, k]_q, \quad (17)$$

which gives the following result.

Corollary 5.4 *All the lower bounds on $LCD[n, k]_q$ given in [7] are also lower bounds on $LCD[n, k]_R$.*

6 Conclusion and Open Problems

In this paper, LCD codes and formally self-dual codes were considered over the ring $R = \mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$, where $v^3 = v$, for q odd. Conditions were given on the existence of LCD codes, and constructions presented for LCD and formally self-dual codes over R . Some of the results presented can easily be generalized to codes over some Frobenius rings such as those in [25]. As an extension of the results in [7], we gave bounds on LCD codes over \mathbb{F}_q , and used these to obtain bound on LCD codes over R . It was shown that lower bounds on LCD codes over \mathbb{F}_q are also lower bounds on LCD codes over R . LCD codes were constructed from weighing matrices. It will be interesting to construct LCD codes from other combinatorial objects. Further, it should be possible to obtain a linear programming bound for codes over R .

Acknowledgements

The authors would like to thank reviewers as well as Professors R. K. Bandi, S. Dougherty, A. Kaya and I. Kotsireas for their useful comments which improved considerably the paper. This research is supported by National Natural Science Foundation of China (61672036),

Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University(2015D11) and Key projects of support program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

References

- [1] Arasu, K.T., Gulliver, T.A.: Self-dual codes over \mathbb{F}_p and weighing matrices. *IEEE Trans. Inf. Theory*, 47(5), 2051–2056 (2001)
- [2] Batoul, A., Guenda, K., Kaya, A., Yildiz, B.: Cyclic isodual and formally self-dual codes over $\mathbb{F}_q + v\mathbb{F}_q$. *Eur. J. Pure Appl. Math.*, 8(1) 64–80 (2015)
- [3] Bennenni, N., Guenda, K., Gulliver, T.A.: Greedy Construction of DNA Codes and New Bounds, accepted to appear at AAECC
- [4] Carlet, C., Guilley, S.: Complementary dual codes for counter-measures to side-channel attacks. In: Pinto, R., Rocha Malonek, P., Vettori, P. (eds) *Coding Theory and Applications*. CIM Series in Mathematical Sciences, 3. Springer, Cham 97–105 (2015)
- [5] Colbourn, C.J., Dinitz, J.H.: *The Handbook of combinatorial theory*. CRC Press, Boca Raton, FL (2006)
- [6] Dougherty, S.T.: Formally self-dual codes and Gray maps. In: *Proceedings of the International Workshop on Algebraic and Combinatorial Coding Theory*, Pomorie, Bulgaria 136–141 (2012)
- [7] Dougherty, S.T., Kim, J.-L., Ozkaya, B., Sok, L., Solé, P.: The combinatorics of LCD codes: linear programming bound and orthogonal matrices. *Arxiv*. <https://arxiv.org/abs/1506.01955> (2015). Accessed June 2015
- [8] Ezerman, M.F., Grassl, M., Solé, P.: The weights in MDS codes. *IEEE Trans. Inf. Theory*, 57(1) 392–396 (2011)
- [9] Gao, J.: Some results on linear codes over $\mathbb{F}_p + u\mathbb{F}_p + u^2\mathbb{F}_p$. *J. Appl. Math. Comput.*, 47(1) 473–485 (2015)
- [10] Guenda, K., Gulliver, T.A.: Self-dual repeated root cyclic and negacyclic codes over finite fields. In: *Proceedings IEEE International Symposium on Information Theory*, 2904–2908 (2012)
- [11] Guenda, K., Jitman, S., Gulliver, T.A.: Entanglement-assisted quantum codes with good performance. *Designs Codes Cryptogr.*, accepted.

- [12] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. <http://www.codetables.de>. Accessed 19 July 2016
- [13] Hardy, G.H., Wright, E.M.: An introduction to the theory of numbers. 4th Ed. Oxford University Press, London, UK (1965)
- [14] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge Univ. Press, New York, 2003
- [15] Ireland, K.F., Rosen, M.: A classical introduction to modern number theory. Springer-Verlag, New York, NY (1982)
- [16] Jia, Y., Ling, S., Xing, C.: On self-dual cyclic codes over finite fields. *IEEE Trans. Inf. Theory*, 57(4) 2243–2251 (2011)
- [17] Jia, M., Solé, P., Wu, B.: Cyclic codes and the weight enumerator of linear codes over $\mathbb{F}_2 + v\mathbb{F}_2 + v^2\mathbb{F}_2$. *App. Comput. Math*, 12(2) 247–255 (2013)
- [18] Karadeniz, S., Dougherty, S.T., Yiliz, B.: Constructing formally self-dual codes over R_k . *Discrete Appl. Math.*, 167(1) 188–196 (2014)
- [19] Kaya, A., Yildiz, B., Siap, I.: Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p$ and their Gray images. *J. Pure Appl. Algebra*, 218(11) 1999–2011 (2014)
- [20] Lidl, R., Niederreiter, H.: Introduction to finite fields and their applications. Cambridge University Press, Cambridge, UK (1986)
- [21] Liu, X., H. Liu, H.: LCD codes over finite chain rings. *Finite Fields Th. App.*, 34 1–19 (2015)
- [22] Liu, Y., Shi, M., Solé, P.: Quadratic residue codes over $\mathbb{F}_p + v\mathbb{F}_p + v^2\mathbb{F}_p$. In: Koç Ç., Mesnager S., Savaş E. (eds) *Arithmetic of Finite Fields. WAIFI 2014. Lecture Notes in Computer Science*, 9061. Springer, Cham 204–211 (2015)
- [23] Massey, J.L.: Linear codes with complementary duals. *Discrete Math.*, 106/107 337–342 (1992)
- [24] MacWilliams, J.F., Sloane, N.J.A.: The theory of error-correcting codes. North-Holland, Amsterdam (1977)
- [25] Shi, M., Solé, P.: Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + \dots + v^{m-1}\mathbb{F}_q$. In: *Proceedings International Workshop on the Arithmetic of Finite Fields* (2015)
- [26] Shi, M., Yao, T., Alahmadi, A., Solé, P.: Skew cyclic codes over $\mathbb{F}_q + v\mathbb{F}_q + v^2\mathbb{F}_q$. *IEICE Trans. Fund.*, E98-A(8) 1845–1848 (2015)

- [27] Zhu, S., L. Wang, L.: A class of constacyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ and its Gray image. Discrete Math., 311(23-24) 2677–2682 (2011)